Bit Byte IT
Committed to quality IT education & services

Enterprise Network Monitoring and Management BootCamp-2
(Nagios, LibreNMS, NetFlow and Syslog Server)

Md. Mahedi Hasan

System & Network Professional

cse.mahedi@gmail.com | www.Mahedi.me

/in/mahedicse/ | /mahedi.cse

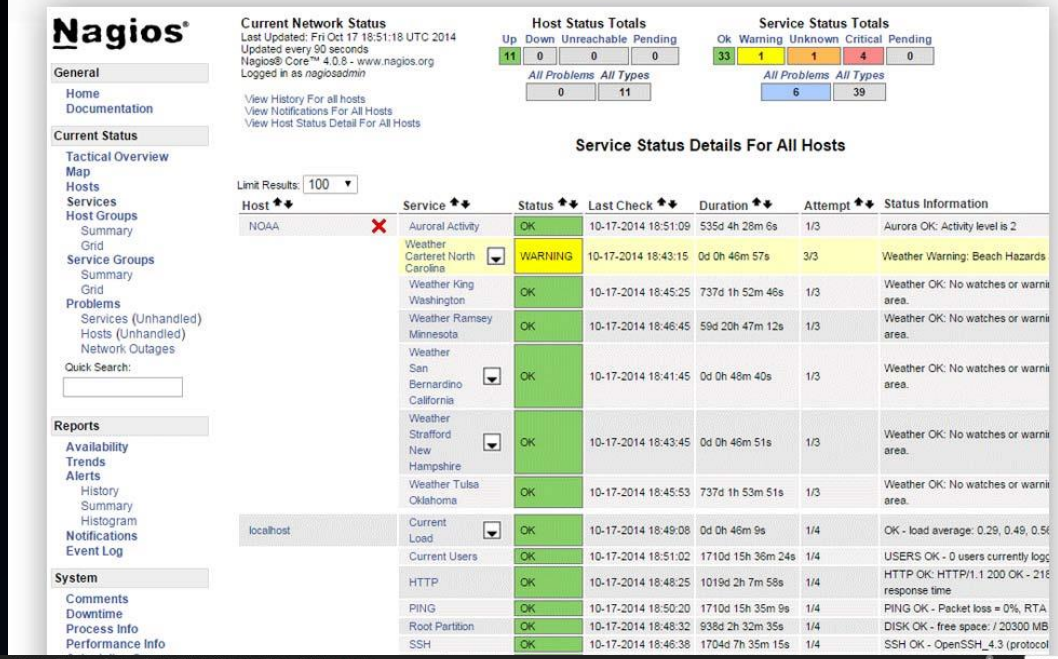
Learning Objective

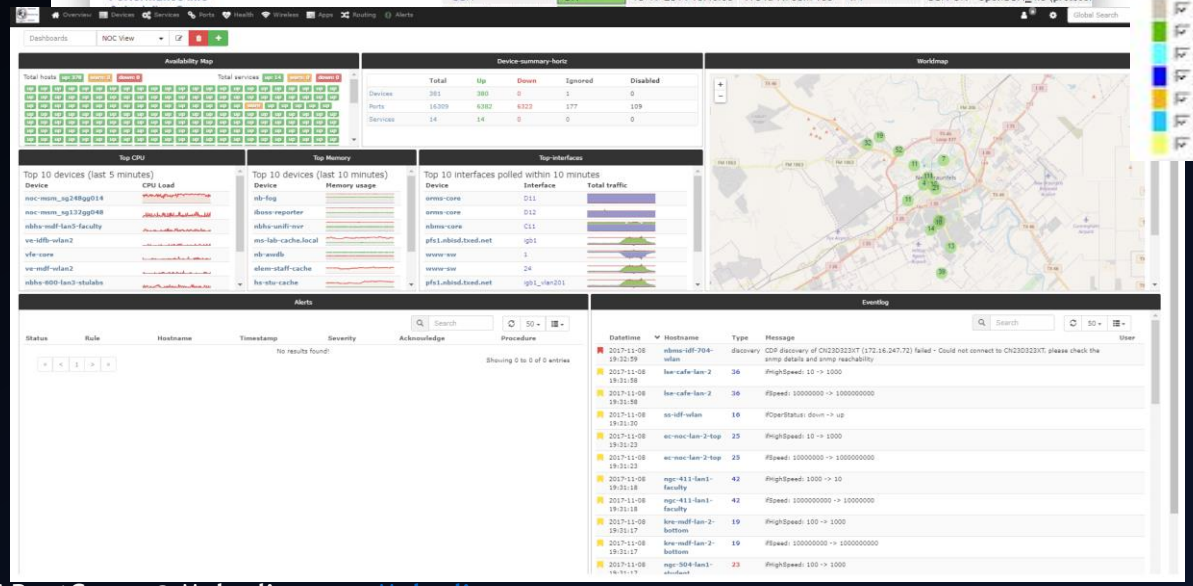
Day-1:

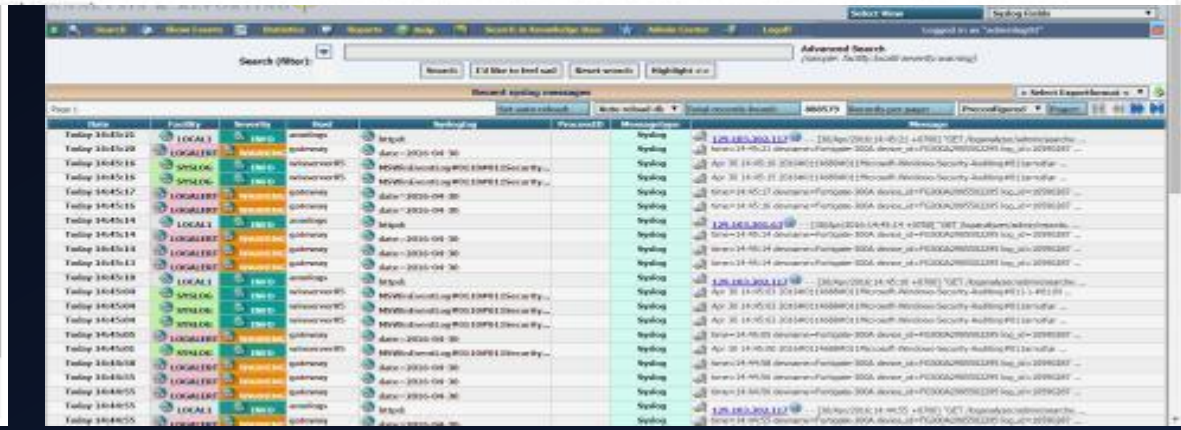
- Details about Network Operation Center (NOC)
- Details about Network Monitoring and Management System (NMS)
- Useful Tools are Using for NMS & NMS best practices
- Details about Agent based and Agent less tools
- Details about SNMP, and its different version of SNMP
- Virtualization and Linux Basic
- Server Lab Setup with VirtualBox/VMware Workstation
- Virtual Server Installation and Networking (CentOS-8)

Network Operation Center (NOC)

Network Monitoring and Management System (NMS)







Useful Tools are Using for NMS & NMS best practices

- Opensource:
  - Cacti
  - Nagios
  - Zabbix
  - LibreNMS
  - Icinga etc.
  - Rsyslog, Log Analyzer
  - NetFlow, nfdump, nFsen
- Paid:
  - ManageEngine
  - SolarWinds
  - Nagios XI etc.

Agent-based Vs Agentless tools

Agent-Based	Agentless
1. Required to install Clients/Agent in every node to monitor	1. No Clients/Agent required to install in nodes
2. Many devices doesn't support to install Clients/Agent	2. Standard protocol use for all tools
3. Provide broader & deeper monitoring beyond what agentless can monitor e.g. richer info than SNMP, CIM, WMI etc. API.	3. Lower maintenance cost (no agent version update / upgrade etc.).
4. Network bandwidth efficiency - data is collected in local node & filter by agent before processed results are forwarded to centralized console	4. Suitable for large nodes deployment.
5. Better security - agent push data to central component instead of letting monitored node for direct remote collection.	5. Less resource usage e.g. CPU in the local node.

Simple Network Management Protocol (SNMP)

- The Simple Network Management Protocol (SNMP) is an Internet Standard protocol defined by the Internet Architecture Board in RFC1157.
- SNMP is used to exchange management information between network devices.
- It is one of the most common protocols used for network management.
- SNMP is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite as defined by the Internet Engineering Task Force
- SNMP generally uses User Datagram Protocol (UDP) port number 161/162. Organizations use SNMP to monitor and manage devices on a local area network (LAN) or wide area network (WAN).
- Most network devices in the market come bundled with SNMP agents
- Currently, there are three major versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3

Components of SNMP

- SNMP manager
  - The SNMP manager is the central system used to monitor the SNMP network. Also known as a network management station (NMS), an SNMP manager is responsible for communicating with the SNMP-agent-implemented network devices. It runs on a host on the network. The manager queries the agents, gets responses, sets variables in them, and acknowledges events from them.
- Managed devices
  - A managed device is an SNMP-enabled network entity that is managed by the SNMP manager. These are usually routers, switches, printers, or wireless devices.
- SNMP agent
  - An SNMP agent is a software process that responds to SNMP queries to provide status and statistics about a network node. SNMP agents play the most important role in management.
  - They are locally located and associated with SNMP network devices from which they collect, store, and transmit monitoring data. Data is transmitted to the designated SNMP manager when queried.

Components of SNMP

- SNMP MIB
  - A management information base (MIB) forms an integral part of network management models.
  - An SNMP MIB is a structure that defines the format of information exchange in an SNMP system. Every SNMP agent maintains an information database describing the parameters of the device it manages. An SNMP manager is a software system that uses SNMP to collect data for fault management, performance management, and capacity planning. SNMP managers store collected data in a MIB as a commonly shared database between the agent and the manager. MIBs are saved as a text file in a specific format that MIB editors, SNMP agent builders, network management tools, and network simulation tools can understand, facilitating network building, testing, deployment, and operations. The managed objects in an MIB are called object identifiers (object IDs or OIDs).
- SNMP OID
  - Object Identifiers (OIDs) are identifiable by strings of numbers separated by dots. There are two types of managed objects:
  - Scalar: Objects defined by a single object instance (i.e. there can only be one result.)
  - Tabular: Objects defined by multiple related object instances that are grouped in MIB tables.

SNMP, and its different versions

- **SNMPv1:**
  - SNMPv1 is the first version of SNMP. It's easy to set up, as it only requires a plain text community.
  - Although it accomplished its goal of being an open, standard protocol, it was found to be lacking in key areas for certain managing applications. For example, it only supports 32-bit counters and has poor security features - a community string is the only security method in the SNMPv1.

SNMP, and its different versions

- SNMPv2c:
  - Designed in 1993, SNMPv2c (where c stands for community) is a sub-version of SNMPv2.
  - SNMPv2c's key advantage over previous versions is the Inform command. Unlike Traps, which are simply received by a manager, Informs are positively acknowledged with a response message. If a manager does not reply to an Inform, the SNMP agent will resend the Inform.
    - Other advantages include:
    - Improved error handling
    - Improved SET commands
  - SNMPv2 security, just like for SNMPv1, comes into the form of community strings. This is a password that your devices will need to able allowed to talk to each other and transfer information when SNMP requests occur

SNMP, and its different versions

- SNMPv3:
  - SNMPv3 is the newest version of SNMP. Its management framework features primarily involve enhanced security.
  - The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control.
  - SNMPv3 supports the SNMP "Engine ID" Identifier, which uniquely identifies each SNMP entity. Conflicts can occur if two entities have duplicate EngineID's. The EngineID is used to generate the key for authenticated messages.
  - SNMP v3 security models come primarily in 2 forms: authentication and encrypting.
  - Authentication:
    - Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the EngineID of the entity. The key is shared with the intended recipient and used to receive the message.
  - Encrypting
    - Privacy encrypts the payload of the SNMP message to ensure that it cannot be read by unauthorized users. Any intercepted traps will be filled with garbled characters and will be unreadable. Privacy is especially useful in applications where SNMP messages must be routed over the Internet.
  - The SNMPv3 protocol also facilitates the remote configuration of the SNMP agents

Thank You

?